UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/586,064 | 06/02/2000 | George T. Hutchings | GIC-599 | 6333 |

7590 03/18/2004

Barry R Lipsitz
Law Offices of Barry R Lipsitz
755 Main Street Building No 8
Monroe, CT 06468

| EXAMINER | |
|---|---|
| TRAN, TONGOC | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | 8 |

DATE MAILED: 03/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/586,064 | HUTCHINGS ET AL. | |
| | Examiner | Art Unit | |
| | Tongoc Tran | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *07 January 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20 and 24-28* is/are rejected.

7)☒ Claim(s) *20-23* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. This office action is in response to applicants' amendment filed on 1/7/2004. Claims 1-28 are pending.

### *Response to Arguments*

2. Applicants contend that the cited prior art, Son, does not disclose:

providing conditional access data to user terminals in two different formats to enable different types of user terminals to decrypt the same encrypted data (page 3, 2rd paragraph and page 4, 2rd paragraph). In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e. "providing conditional access data to user terminals in two different formats to enable different types of user terminals to decrypt the same encrypted data") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Applicants recites in item (c ) "providing a data stream comprising the at least one encrypted data service and first and second CA data to user terminals, including at least a first user terminal that is compatible with the first CA data, and a second user terminal that is compatible with the second CA data". Son discloses at least one encrypted data service, for example, col. 3, lines 42-48, video program is encrypted by a video on-demand source (CAP)), first and second CA data to user terminals, including at least a first user terminal that is compatible with the first CA data, and a second user terminal that is compatible with the second CA data, for example, col. 2, lines 33-38,

plurality of subscriber stations, col. 2, lines 52-54, subscriber stations may be, for example, set-top boxes and associated television equipment for viewing the video content by end users). Son's second distribution center or remote server (second CAP) provides first and second CA data for first and second subscriber station, the CA data has to be compatible with the user terminals. In item (b), the claim language refers the second CA data to be "in a different, second format for successive crypto-periods". This limitation is met by Son's teaching when the remote server decrypt the encrypted format from the video on-demand source and then re-encrypted with a different format and send to the requested subscriber station, for example, col. 3, lines 49-59. Applicants further stated that Son only teach one conditional access provider (CAP), the video on-demand source, and the server of Son is not a secondary CAP because the server does not provide second conditional access data in response to the first conditional access data. Examiner disagrees. Son teaches at least one video on-demand source (primary CAP) and at least a second distribution center or remote server (second CAP) wherein the server provide second conditional access data in response to the first conditional access data, for example, col. 5, lines 6-15 (server received encrypted data from source, decrypt and re-encrypt data into second form).

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6, 10-14, 16, 18-24 and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Son et al. (U.S. Patent No. 6,229,895 hereinafter Son) in view of Fruehauf et al. (U.S. Patent No. 6,590981 hereinafter Fruehauf).

In respect to claim 1, Son discloses a method for enabling a primary conditional access provider (CAP) and at least one secondary CAP to provide conditional access (CA) data in respective different formats to control access to at least one data service, comprising the steps of (see Fig. 1-6):

(a) providing, at the primary CAP, first CA data in a first format for encrypting the at least one data service during a plurality of successive crypto-periods, and time data for identifying the successive crypto-periods (see Fig. 1-6 and col. 5, lines 1-35);

(b) providing the first CA data and the time data from the primary CAP to the at least one secondary CAP; wherein the at least one secondary CAP is responsive to the first CA data and time data for providing second CA data in a different, second format for the successive crypto-periods (see col. 5, lines 15-35); and

(c) providing a data stream comprising the at least one encrypted data service and first and second CA data to user terminals, including at least a first user terminal that is compatible with the first CA data, and a second user terminal that is compatible with the second CA data (see col. 5, lines 35-50). Son does not explicitly disclose providing a time data for identifying the successive crypto-period. However, Fruehauf discloses a time data for identifying the successive crypto-period (see col. 6, lines 39-59). Therefore, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to incorporate Son's teaching of providing at the primary CAP first CA data with Fruehauf's teaching of providing a time data for identifying the successive crypto-period for the purpose of determining when the synchronization time need to be readjusted if the cryptographic processing time exceed a predetermined limit (see Fruehauf col. 6, lines 53-59).

In respect to claim 2, Son and Fruehauf disclose the method of claim 1. Fruehauf further teaches wherein the time data indicates respective start times of the crypto-periods (see col. 6, lines 39-59, at any given time).

In respect to claim 3, Son and Fruehauf disclose the method of claim 2. Fruehauf further discloses wherein the time data designates absolute times of the crypto-periods (see col. 6, lines 39-59, a predetermined limit).

In respect to claim 4, Son and Fruehauf disclose the method of claim 2. Fruehauf further discloses wherein the time data designates relative times of the crypto-periods in relation to a reference time of the at least one data service (see col. 6, lines 39-59, at any given time).

In respect to claim 5, Son and Fruehauf disclose the method of claim 1. Fruehauf further discloses wherein the time data is a lead time of at least one crypto-period (see col. 6, lines 39-59, at any given time).

In respect to claim 6, Son and Fruehauf disclose the method of claim 5. Fruehauf further discloses wherein the lead time is responsive to a required processing time of the at least one secondary CAP (see col. 6, lines 39-59, at any given time).

In response to claim 10, Son and Fruehauf disclose the method of claim 1. Son further discloses the first CA data is streamed in real-time from the primary CAP to the at least one secondary CAP without being requested therefrom (see col. 3, lines 21-47).
In respect to claim 11, Son and Fruehauf disclose the method of claim 10. Son further discloses wherein the at least one secondary CAP provides its second CA data essentially in real-time after receipt of the first CA data and time data thereat (see col. .3, lines 37-47).

In respect to claim 12, Son and Fruehauf disclose the method of claim 1. Son further discloses comprising the further steps of storing the first and second synchronized CA data and the at least one encrypted data service for subsequent retrieval to provide said data stream (see col. 3, lines 42-47). Fruehauf further discloses synchronizing the first CA data and the second CA data with the at least one encrypted data service (see col. 6, lines 39-59).

In respect to claim 13, Son and Fruehauf disclose the method of claim 12. Son further discloses comprising the further step of retrieving the first and second synchronized CA data and the at least one encrypted data service to provide said data stream in response to a user request (see col. 3, lines 49-59).

In response to claim 14, Son and Fruehauf disclose the method of claim 13. Son further discloses wherein the user request is provided as part of a video-on -demand service (see col. 4, lines 49-59).

In response to claim 16, Son and Fruehauf disclose the method of claim 1. Son further discloses wherein the first CA data is provided from the primary CAP to the at

least one secondary CAP via a CA data delivery network (see col. 2, lines 1-30, cable distribution network).

In respect to claim 18, Son and Fruehauf disclose the method of claim 1. Son further discloses wherein the first and second CA data are provided to a message insertion subsystem in-band with the encrypted data service to form said data stream (see col. 2, lines 1-30, cable distribution network).

In response to claim 19, Son and Fruehauf disclose the method of claim 1. Son further discloses wherein the first CA data and the time data are provided from the primary CAP to a plurality of secondary CAPs, each of which is responsive to the first CA data for providing CA data in different, respective formats for the successive crypto-periods (see col. 5, lines 1-35); the data stream comprises the CA data in the different, respective formats; and the user terminals include respective user terminals that are compatible with the different, respective formats (see col. 5, lines 36-50).

In respect to claim 20, Son and Fruehauf disclose the method of claim 1. Son further discloses wherein the first CA data and encrypted data service are provided in a first data stream from the primary CAP to the at least one secondary CAP for insertion of the second CA data, and a corresponding second data stream is returned to the primary CAP for formation of said data stream that is provided to the user terminals (see col. 5, lines 1-56).

Claims 21-23 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

In respect to claim 24, Son and Fruehauf disclose the method of claim 20. Son further discloses wherein the second data stream is formed by overwriting the first CA data with corresponding second CA data in corresponding packets of the first data stream (see col. 5, lines 5-15).

In response to claim 26, Son and Fruehauf disclose the method of claim 1. Son further discloses wherein the primary CAP first and at least one secondary CAPS are provided at a headend (see col. 2, lines 40-48).

In respect to claim 27, Son and Fruehauf disclose the method of claim 1. Son further discloses wherein the first CA data is provided from the primary CAP to the at least one secondary CAP in an encrypted form, comprising the further step of: providing data to the at least one secondary CAP for decrypting the encrypted first CA data (see col. 3. lines 35-40).

In respect to claim 28, the claim limitations is an apparatus claim that is substantially similar to method claim 1 and therefore the same rejection applied.

4. Claim 7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Son et al. (U.S. Patent No. 6,229,895 hereinafter Son) in view of Fruehauf et al. (U.S. Patent No. 6,590981 hereinafter Fruehauf) as applied to claim 6 above, and further in view of Okamoto et al. (U.S. Patent No. 5,944,794 hereinafter Okamoto).

In respect to claim 7, Son and Fruehauf disclose the method of claim 5. Son further discloses wherein the first CA data is provided to the at least one secondary CAP in successive packets, each packet comprising first CA data and time data for a

plurality of crypto-periods (see col. 3, line 49-col. 4, line 10). Both Son and Fruehauf do not explicitly disclose transmitting time data for a plurality of crypto-period. However, Okamoto discloses transmitting time data for a plurality of crypto-period (see col. 15, lines 1-8 and col. 22, line 66-col. 23, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Son's teaching of transmitting CA data from primary CAP to secondary CAP with Okamoto's teaching of including time data to carry out authentication process for the benefit of judging the success of an authentication process.

In respect to claim 8, Son and Fruehauf disclose the method of claim 7. Son further disclose wherein the plurality of crypto-periods comprise a current crypto-period and future crypto-periods (see col. 3, lines 49-65).

5. Claims 9, 15, 17 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Son et al. (U.S. Patent No. 6,229,895 hereinafter Son) in view of Fruehauf et al. (U.S. Patent No. 6,590981 hereinafter Fruehauf) as applied to claim 6 above, and further in view of Pinder et al. (U.S. Patent No. 6,105,134 hereinafater Pinder).

In response to claim 9, Son and Fruehauf disclose the method of claim 1. Both Son and Fruehauf do not explicitly disclose wherein the first CA data comprises a control word for each of the crypto-periods. However, Pinder discloses using control words as a key for each of the crypto-periods (see col. 8, line 64-col. 9, line 24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to implement the control word as a key for a more secure data transfer because a control word a short term key and is generated by a random number generator (see col. 9, line 1-3 and 11-12).

In respect to claim 15, Son and Fruehauf disclose the method of claim 1. Son and Fruehauf do not disclose wherein the primary CAP provides a program identifier to the at least one secondary CAP to inform the at least one secondary CAP that the first CA data associated with the at least one data service. However, Pinder discloses a packet identifier (PID) that are carrying information for a given subcategory will have a same PID (see col. 19, lines 9-40). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Pinder's teaching of packet identifier with Son's teaching of packet transferring between primary CAP and secondary CAP in order to ensure that CA data sent from the primary CAP is corresponds to the correct data service being transferred (see col. 19, lines 11-16).

In respect to claim 17, Son and Fruehauf disclose the method of claim 1. Son and Fruehauf do not disclose but Pinder discloses wherein the first and second CA data are provided to a message insertion subsystem out-of-band from the encrypted data service to form said data stream (see col. 7, lines 26-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Son's first and second CA data from the encrypted data service to form a data stream with the teaching of Pinder sending out-of-band for the benefit of providing a wider distribution of channel (i.e. Internet) (see col. 8, lines 47-49).

In respect to claim 25, Son and Fruehauf disclose the method of claim 1. Son and Fruehauf do not explicitly disclose but Pinder discloses wherein the first CA data comprises entitlement control messages (ECM) (see col. 4, lines 14-36). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the entitlement control message taught by Pinder with Son's secure program data transmission between first and second CAP for a more secure data protection because contain information needed to decrypt the encrypted portion of the

***Allowable Subject Matter***

6. Claims 21-23 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

In respect to claim 21, prior does not teach method claim 20, comprising the further steps of:

Retaining a copy of the first data steam at the primary CAP;

Filtering at the primary CAP, the second data steam that is returned form the at least one secondary CAP to recover the second CA data; and

Combining the recovered second CA data with the retrained copy of the first data stream to form said data steam that is provided to the user terminals.

In respect to claim 22, prior art does not teach the method of claim 20, comprising the further steps of :

Retaining a copy of the first data steam to determined a deviation therebetween.

In respect to claim 23, prior art does not teach the method of claim 22, comprising the further step of:

If the deviation is detected, using the retained copy of the first data stream, which does not contain the second CA data, to form said data stream that is provided to the user terminals.

associated instant data (see col. 4, lines 29-31).

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

TT
March 16, 2004

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137